آشنایی با جنگ نرم

جنگ سایبر (۲)

تدوین و گرد آوری :

مهندس محمد ابراهیم‌نژاد

حمید اسکندری

سرشناسه : ابراهیم‌نژاد شلمانی، محمد، ۱۳۵۶ - گردآورنده
عنوان و نام پدیدآور : آشنایی با جنگ نرم/ جنگ سایبر-تدوین و گردآوری محمد ابراهیم‌نژاد، حمید اسکندری.
مشخصات نشر : تهران: بوستان حمید، ۱۳۹۰-
مشخصات ظاهری : ج.: مصور ، جدول ، نمودار.
شابک : دوره: ۴-۱-۹۲۲۹۳-۶۰۰-۹۷۸ ؛ ج.۲: ۲-۰۹-۶۴۱۲-۶۰۰-۹۷۸
وضعیت فهرست نویسی: فیپا
یادداشت : ج. ۲ (چاپ اول : ۱۳۹۰) (فیپا).
مندرجات : ج. ۱ و ۲. جنگ سایبر
موضوع : جنگ نرم
موضوع : جنگ اطلاعاتی
موضوع : تروریسم رایانه‌ای
شناسه افزوده : اسکندری، حمید، ۱۳۳۸ - گردآورنده
رده بندی کنگره : ۲۷۵UB / الف۱۵ آ ۵ ۱۳۹۰
رده بندی دیویی : ۳۴۳/۳۵۵
شماره کتابشناسی ملی : ۲۲۹۸۲۶۶

انتشارات

عنوان : آشنایی با جنگ نرم - جنگ سایبر (۲)
تدوین و گرد آوری: محمد ابراهیم نژاد - حمید اسکندری
ناشر : بوستان حمید
نوبت چاپ : چاپ اول (زمستان ۱۳۹۰)
شمارگان : ۲۰۰۰
قیمت : ۷۵۰۰ تومان

تلفن ناشر: ۳۳۷۰۰۹۲۷ صندوق پستی ۳۳۱- ۱۷۷۷۵

پیش گفتار

جنگ نرم در برابر جنگ سخت در حقیقت شامل هر گونه اقدام روانی و تبلیغات رسانه‌ای می‌شود که جامعه هدف یا گروه هدف را نشانه می‌گیرد و بدون درگیری نظامی و گشوده شدن آتش رقیب را به انفعال یا شکست وا می‌دارد. جنگ روانی، جنگ رایانه‌ای، جنگ اینترنتی، براندازی نرم، راه‌اندازی شبکه‌های رادیویی و تلویزیونی و شبکه‌سازی از اشکال جنگ نرم هستند (سایت قوه مقننه، ۱۳۸۷)

هدف از تدوین این سری کتاب ها آشنایی با ابعاد مختلف جنگ نرم بوده که سعی می شود در جلد های اولیه به جنگ سایبر و تهدیدات در فضای مجازی و اینترنت پرداخته شود. در ابتدای مقدمه کتاب، به مستندات قانونی و مواردی از راهبرد های حفاظتی و امنیتی فضای سایبر از منظر پدافند غیرعامل اشاره می گردد:

در بند ۱۱ سیاست‌های کلی نظام در خصوص پدافند غیرعامل (ابلاغ شده) این چنین آمده است: [۱]

« اصول و ضوابط مقابله با تهدیدات نرم‌افزاری و الکترونیکی و سایر تهدیدات جدید دشمن به منظور حفظ و صیانت شبکه‌های اطلاع‌رسانی، مخابراتی و رایانه‌ای.»

مواردی از راهبرد ها[۲]

۱- نهادینه سازی فرامین و قانون مند سازی تدابیر مقام معظم رهبری در خصوص پدافند غیرعامل

۲- توسعه امنیت ، ایمنی و پایداری در شبکه های ارتباطی با تأکید بر فن آوری بومی

---

[۱] - این سیاست‌ها که در ۱۳ بند به تصویب رسیده و با تأیید مقام معظم رهبری ابلاغ شده است.

[۲] - پدافند غیرعامل در حوزه سایبر – شرکت ایزایران – مرکز پدافند غیرعامل.

۳- نهادینه کردن اصول و ملاحظات پدافندغیرعامل در طرح های توسعه شبکه ها

۴- بهره مندی از شبکه ارتباطی ویژه مدیریت کشور در شرایط بحران

۵- حمایت از برنامه ایجاد شبکه ملی اینترنت مبتنی بر مؤلفه های امنیت ، ایمنی ، پایداری و متکی برفن آوری های بومی

۶- توسعه توان کنترل و مدیریت بحران و برنامه های حراست، حفاظت و ضد جاسوسی.

قدرت‌های سلطه‌گر برای فراهم‌سازی زمینه‌های تهاجم و تجاوز از رویه‌ها، مهارت‌ها و فناوری‌های نرم سود می‌جویند که در همگرایی با فناوری‌های سخت، بستر لازم برای چنین حملاتی را فراهم می‌سازد.

جنگ سایبری را می‌توان به صورت کلی تحت عنوان حمله عمدی به زیر ساخت‌های اطلاعاتی دشمن از طریق استفاده از تکنیک‌های نفوذگری به رایانه ها در عین جلوگیری کامل از (یا مشکل کردن) انجام اقدامات مشابه از طرف دشمن تعریف نمود.

در مقدمه اخبار با اهمیت در خصوص جاسوس افزار « **استاکس نت** » بیان می گردد:

به گزارش پایگاه اطلاع‌رسانی وزارت صنایع ومعادن ایران[۳] ، دبیر شورای فناوری اطلاعات وزارت صنایع و معادن در مورد ویروس" استاکس نت" گفت: اگر مدیران صنعتی از دانش فنی لازم در این خصوص برخوردار بودند ما شاهد شیوع این ویروس در واحدهای صنعتی نبودیم و چه بسا می‌توانستیم حمله این جاسوس افزار را در نطفه خفه کنیم.

ایشان درخصوص آسیب‌های احتمالی ناشی از نفوذ ویروس به سیستم‌های صنعتی، تصریح کرد: خروج اطلاعات مربوط به میزان تولید، نحوه فعالیت خط تولید و حتی بروز اختلال در روند تولید از جمله آسیب‌های احتمالی ناشی از نفوذ ویروس است که در

---

[۳] - اتاق خبر روابط عمومی - ۱۳ شهریور ۱۳۸۹

صورت عدم جلوگیری، هزینه‌های جبران ناپذیری را به صنعتگران تحمیل خواهد کرد.

مدیر کل صنایع برق، الکترونیک و فناوری اطلاعات وزارت صنایع و معادن از شناسایی ۳۰ هزار IP صنعتی آلوده به جاسوس افزار «استاکس نت» خبر داد و گفت: این ویروس، اطلاعات مربوط به خطوط تولید را به خارج از کشور منتقل می‌کند. هدف‌گیری این ویروس در راستای اهداف تحریم و جنگ الکترونیکی (سایبری) علیه ایران است.

وی با بیان اینکه واحدهای صنعتی کشور دیر متوجه نفوذ جاسوس افزار به سیستم‌های خود شده‌اند، افزود: میزان آلودگی سیستم‌ها مشخص شده و حدود ۳۰ هزار IP در کشور شناسایی شده که به این ویروس جاسوس آلوده‌اند. وی با بیان اینکه سیستم های صنعتی به آنتی ویروس خاص برای مبارزه با جاسوس افزار مجهز خواهند شد، گفت: سیستم‌های اتوماسیون صنعتی که در ایران و بسیاری از کشورها تحت برند اسکادا شرکت زیمنس تولید شده‌اند هدف اصلی این جاسوس افزار هستند.

لذا به کلیه مدیران و کارشناسان دستگاه های اجرایی کشور توصیه می شود دانش و آگاهی خود را در حوزه ماهیت تهدیدات نوین بر علیه زیرساخت های مراکز ثقل توسعه داده و بر اساس آن طرح های توسعه ای خود را تدوین نمایند.

با توجه به اهمیت و کاربردی بودن موضوع در سطوح مختلف اقشار جامعه تصمیم گرفته شد تا مباحث جنگ نرم بخصوص جنگ در فضای سایبر و امنیت رایانه با استفاده از منابع معتبر و بروز به صورت سری کتاب های مستقل تدوین گردد و متخصصین و کارشناسان بر اساس نیاز و علاقه، آن ها را تهیه نمایند. بدون شک مورد استفاده مخاطبین و علاقه مندان در این حوزه قرار خواهد گرفت.

با تشکر

مؤلفین

فهرست مطالب

مقدمه

در حال حاضر، اینترنت به تنهایی توسط بیش از یک میلیارد نفر مورد استفاده قرار می‌گیرد و تقریبا در تمامی کشورها ،سازمان ها و افراد به یکدیگر از طریق اینترنت، متصل می‌باشند. بنابراین مردم علاقه زیادی به داشتن فضا رایانه‌ای امن و بی خطر دارند. با این وجود، فضا رایانه‌ای به طور اعم و اینترنت به طور اخص نسبت به رویدادهای ناخوشایند و در حال گسترش و نیز تهاجم توسط طیف وسیعی از نفوذ گرها[۴]، خلافکاران و خرابکاران که به زیر ساخت ها دسترسی دارند، آسیب پذیر می‌باشند. بسیاری از مردم و سازمان‌هایی که به طور فزاینده ای متکی به فضا رایانه‌ای هستند، از میزان آسیب پذیری و بی دفاع بودن خود، بی خبر می‌باشند و بسیاری از استفاده کنندگان و کاربران این فضا، از آموزش ضعیف و تجهیزات ناکافی، برخوردار هستند.

در نهایت، جامعه انتظار دارد تا سامانه‌های رایانه‌ای، قابل اعتماد گردیده و اینکه بتوانند علیرغم اختلال های موجود، خطاهای کاربر و استفاده کننده و تهاجم رایانه‌ای طرف‌های متخاصم، به کار خود با رایانه ادامه دهند و همچنین نیاز نباشد که اقدامات دیگری را انجام دهند. اعتماد سازی دارای ابعاد زیادی شامل صحت، اعتبار، ایمنی، ماندگاری و نیز امنیت می‌باشد.

حملات سایبر متوجه اهدافی است که ارزش رسانه‌ای بالایی داشته باشند: حملات سایبر به طریقی دنبال می‌شوند که خسارات حاصله به حداکثر برسد و موج رسانه‌ای گسترده‌ای تولید شود. واحدها و تأسیسات دولتی و نظامی و شرکت‌های چندملیتی در لیست اهداف قرار دارند.

---

[۴] .Hackers

اغلب حملات از طریق نقایص و امکانات موجود در فضای فناوری اطلاعات هدایت می‌شود. قسمت ذیل امکاناتی را که ممکن است بعنوان اهداف اولیه حمله‌کننده‌ها قرار گیرد، ارائه می‌دهد:

پورتال‌های کاربری، برنامه‌های کاربردی هستند که اغلب نیازهای روزمره یک کاربر را در ارتباط با جهان خارج پوشش می‌دهند. این شامل برنامه‌هایی از قبیل پست الکترونیک،کاوشگرهای وب، ابزارهای چت، نرم افزار کنترل راه دور، نرم افزار مبتنی بر شبکه و حوزه‌ای از نرم افزارهای مشابه می‌باشد. حمله‌کننده‌ها از امکانات موجود علیه خود سیستم میزبان بهره‌گیری می‌نمایند و یا از آنها در حمله به سیستم دیگر بهره می‌گیرند. اتاق‌های گفتگوی آنلاین و برنامه‌های کاربردی تحت وب همگی از امکاناتی هستند که در صورت دقت نکردن در مورد استفاده از آنها ممکن است به عنوان ابزارهایی در دست مهاجمین سایبر قرار گیرند. فایل‌های به روزرسانی نیز از جمله مواردی هستند که در نصب آنها حداکثر دقت باید صورت پذیرد.

حمله‌کنندگان با استفاده از مکانیزم‌ها و ابزار فوق اقدام به تزریق کدهای آلوده‌ای به رایانه میزبان می‌نمایند که بصورت فایل‌های اجرایی مخفی نیازهای برنامه‌ریزی شده آنها را چه در قالب جمع‌آوری اطلاعات و چه برقراری امکان کنترل رایانه قربانی یا وارد آوردن صدمه به آن، تأمین می‌نمایند.این بسته‌های آلوده شامل ویروس‌ها، کرم‌ها، تروجان‌ها و اسکریپت‌های اجرایی می باشند که هرکدام از این‌ها به همراه مکانیزم آنها در قالب فصول مربوطه در این کتاب بحث خواهند شد.

مکانیزم‌های مذکور، روش‌های نفوذ خارجی مستقیم به سیستم‌ها و روش‌های علمی و عملی پیشرفته مقابله با آنها، همگی مطالبی هستند که درفصول مختلف این کتاب توصیف شده و مراجع معتبر و مناسبی برای کسب اطلاعات در این حوزه‌ها ارائه می‌گردد.